

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.




# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/623,488	10/30/2000	Feng Bao	P19949	7274
7055	7590	08/04/2004	EXAMINER	
GREENBLUM & BERNSTEIN, P.L.C. 1950 ROLAND CLARKE PLACE RESTON, VA 20191			PARTHASARATHY, PRAMILA	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 08/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/623,488	<b>Applicant(s)</b> BAO ET AL. 	
	<b>Examiner</b> Pramila Parthasarathy	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 30 April 2004.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 8-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 8-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date: _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                    | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date: _____ | 6) <input type="checkbox"/> Other: _____  |

### ***DETAILED ACTION***

1. This action is in response to request for reconsideration filed on March 19, 2004. Original application contained Claims 1 – 7. Applicant cancelled claims 1- 7 and added Claims 8 – 18. Therefore, presently pending claims are 8 – 18.

### ***Response to Arguments***

2. Applicant's arguments filed on March 19, 2004, have been fully considered but they are not persuasive for the following reasons:

Regarding independent claim 8, applicant argued that the cited prior arts (CPA) [Micali U.S. Patent 5,666,420 and Angebaud et al. 5,218,637] do not teach, suggest or disclose, "authentication certificate", "the first party sending the encrypted first digital data and the authentication certificate to the second party", "the second party verifying that the encrypted first digital data is an encryption of the first digital data as an encryption of the first digital data using the authentication certificate", "the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data", or "the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party is valid". These arguments are not found persuasive.

Micali teaches a communication method between a first party and a second party exchanging digital signature suitable for message authentication (Column 5 lines 46 – 48 and Column 9 lines 4 – 14). Micali teaches that the first party sending the encrypted first digital data and authentication certification to the second party (Column 3 line 61 – 27 and Column 5 lines 46 – 48). Micali teaches that the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data and that the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data (Column 4 lines 21 – 28 and Column 5 lines 46 – 62).

Micali suggests that once the identities are verified and contact is established, the digital data could be exchanged (Column 11 lines 25 – 67). Micali does not explicitly teach that the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party is valid. However, Angebaud teaches and describes a method for exchange of two digital certificates wherein, the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party is valid (Column 9 lines 30 – 61).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the established secure communication to send unencrypted digital data as taught by Angebaud, after the authentication certification is verified through exchange of digital signature as taught by Micali.

Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner respectfully asserts that CPA does teach or suggest the subject matter broadly recited in independent claim 8. Dependent claims 9 – 18 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action. Accordingly, rejections for claims 8 – 18 are respectfully maintained.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 8 – 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Micali (U.S. Patent No. 5,666,420) in view of Angebaud et al. (U.S. Patent No. 5,218,637 hereinafter "Angebaud"). Regarding Claim 1, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67), the method comprising:

the first party encrypting the first digital data and generating an authentication certificate, the authentication certificate authenticating that the encrypted first digital

data is an encryption of the first digital data, and sending the encrypted first digital data and the authentication certificate to the second party (Column 5 Lines 46 – 48 and Column 9 lines 4 – 14);

the second party verifying that the encrypted first digital data is an encryption of the first digital data using the authentication certificate, and the second party sending the second digital data to the first party when the encrypted first digital data is an encryption of the first digital data (Column 9 lines 50 – 51);

the first party verifying that the second digital data is valid and, when the second digital data is valid, the first party accepting the second digital data and sending the unencrypted first digital data to the second party (Column 5 lines 52 – 54);

the second party verifying that the unencrypted first digital data is valid, and when the unencrypted first digital data is valid, the second party accepting the unencrypted first digital data and, when the unencrypted first digital data is invalid, the second party sending the encrypted first digital data and the second digital data to a third party, the third party having a decryption key to decrypt the encrypted first digital data (Column 5 lines 55 – 62); and

the third party receiving the encrypted first digital data and the second digital data from the second party when the unencrypted first digital data is invalid, the third party decrypting the encrypted first digital data to obtain the decrypted first digital data, verifying that the decrypted first digital data and the second digital data are valid and, when the decrypted first and the second digital data are valid, sending the decrypted

first digital data to the second party and the second digital data to the first party (Column 5 lines 63 - 67).

Micali does not explicitly disclose that the first party sending the unencrypted first digital data after the first party verifies that the second digital data from the second party is valid. However, in an analogous environment, Angebaud discloses a method of exchanging digital data between a first party having a unique first digital data and a second party having a unique second digital data over a communication link (Angebaud Column1 lines 12 – 14) and also discloses the method comprising a – d (Column 9 lines 29 – 51).

- a) the first party sending the encrypted first digital data to the second party;
- b) the second party verifying that the encrypted first digital is an encryption of the first digital data and second party sending the second digital data to the first party;
- c) the first party verifying that the second digital data is valid and sends the unencrypted first digital data to the second party;
- d) the second verifying that the first digital data is valid, accepts the first digital data.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was made to use the established secure communication to send unencrypted digital data as taught by Angebaud and suggested by Micali, after the authentication certification is verified through exchange of digital signature as taught by Micali. Such modifications would have been obvious because by combining the teachings of Micali with Angebaud, the first and second parties can keep the parallel



accreditations in each exchange to an absolute minimum and the need to authenticate the unencrypted data could be eliminated.

Claim 9 is rejected above in rejecting claim 8. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67), in which

the first and second digital data are on files M\_A and M\_B respectively, the first party encrypting the first digital data on a concatenation of file M\_A and a one-way hash of file M\_B; and, when the encrypted first digital is an encryption of the first digital data, the second party encrypting the second digital data on a concatenation of file M\_B and a one-way hash of file M\_A (Column 5 lines 58 – 59 and Column 8 lines 51 – 68);

Claim 10 is rejected above in rejecting claim 8. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67), wherein

the first and second digital data are digital signatures belonging to the first and second party, respectively (Col.4 Line 66 and Col.3 Lines 62 – 63 and Col.4 Lines 14 – 34).

Claim 11 is rejected above in rejecting claim 8. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67), wherein

the second digital data is a file secret file M which the first party wishes to receive from the second party in exchange for the first digital data (Col.5 Lines 46 – 53). Micali does not explicitly disclose that the file M is a secret file. However, Angebaud discloses that the second digital data is a secret file M which the first party wishes to receive from the second party in exchange for the first digital data (Angebaud Column 1 lines 12 – 14 and Column 9 lines 34 – 61).

Claim 12 is rejected above in rejecting claim 8. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67),

wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (Column10 lines 50 – 65).

Claim 13 is rejected above in rejecting claim 12. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67),

Wherein the digital signature schemes are discrete logarithm based schemes; and the public key encryption scheme is a discrete logarithm based scheme (Column 10 lines 50 – 54).

Claim 14 is rejected above in rejecting claim 12. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67), wherein

the public key encryption scheme is a discrete logarithm based scheme (Column 10 lines 50 – 54).

Micali does not disclose the digital signature schemes are Guillou-Quisquater type digital signature schemes. However, Angebaud discloses Wherein the digital signature schemes are Guillou-Quisquater type digital signature schemes (Angebaud Column 7 lines 24 – 68 and Column 8 lines 1 – 45). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for using the Guillou-Quisquater digital signature schemes there by eliminating the need to transfer a secret and/or controlling an action between two parties which establish reciprocal authentication, without a

previously shared secret and without a common cryptographic algorithm. Such modifications would have been obvious because by combining the teachings of Micali with Angebaud, the first and second parties can keep the parallel accreditations in each exchange to an absolute minimum.

Claim 15 is rejected above in rejecting claim 9. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67), wherein

the first and second digital data are digital signatures belonging to the first and second party, respectively (Column 4 line 66 and Column 3 lines 62 – 63 and Column 4 lines 14 – 34).

Claim 16 is rejected above in rejecting claim 9. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67),

wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (Column 10 lines 50 – 65).

Claim 17 is rejected above in rejecting claim 10. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67),

wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (Column 10 lines 50 – 65).

Claim 18 is rejected above in rejecting claim 11. Furthermore, Micali discloses a method of exchanging digital data over a communications link between a first party having a unique first digital data and a second party having a unique second digital data (Column 3 line 36 – Column 11 line 67),

wherein the first party has a pair of public/private keys in a first digital signature scheme; the second party has a pair of public/private keys in a second digital signature scheme; and the third party has a pair of public/private keys in a public key encryption scheme (Column 10 lines 50 – 65).

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or**  
**faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..


Application/Control Number: 09/623,488  
Art Unit: 2136

Page 13

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy  
Patent Examiner  
703-305-8912  
July 26, 2004

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100